element and the selected element. Integrity checksums can also verify communications between the requesting element and the selected element.

The network can be logically partitioned to create at least two separate realms. Each realm is provided with its own network security server and an inter-realm authentication means for communication with another of the at least two separate realms. The realms can share the registration database.

Additionally, the network can be coupled to a dial-up server to permit dial-up users access the network elements through the same network. The dial-up server supports a network communication protocol to connect the dial-up users to the network and a dial-up access protocol to connect the dial-up users to a dial-up access network.

BRIEF DESCRIPTION OF THE FIGURES

The present invention will be described with reference to the accompanying drawings, wherein:

FIG. **1** illustrates a high-level block diagram of a conventional network.

FIG. **2** illustrates a high-level block diagram of a network including a network security server **208** in connection with the present invention.

FIG. **3** illustrates another embodiment of network security in connection with the present invention.

FIG. **4** is a flow diagram illustrating various operations performed in association with servers of network security server **208** in connection with the present invention.

FIG. **5** illustrates an exemplary high level, state diagram of an operational flow in connection with the present invention.

FIG. **6** illustrates a log-in procedure in connection with the present invention.

FIG. **7** illustrates an access request procedure in connection with the present invention.

FIG. **8** illustrates a communication session between the user element and the selected network element in connection with the present invention.

FIG. **9** is a computer environment for implementing various servers and elements in connection with a computer program product for the present invention.

FIG. **10** illustrates a dial-up access network in connection with the present invention.

The preferred embodiment of the invention is described below with reference to these figures where like reference numbers indicate identical or functionally similar elements. Also in the figures, the leftmost digit of each reference number corresponds to the figure in which the reference number is first used.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The preferred embodiment of the invention is discussed in detail below. While specific steps, configurations and arrangements are discussed, it should be understood that this is done for illustrative purposes only. A person skilled in the relevant art will recognize that other steps, configurations and arrangements can be used without departing from the spirit and scope of the invention.

1. Network Security Issues

This section provides an overview of network environment, security concerns and problems, and general mechanisms that address the concerns and solve the problems.

1.1 User and Network Elements

A network consists of a collection of individual systems, primarily network elements and user elements, and a communication network. This communication network interconnects these elements together to form a network of systems that carry out specified functions and offer desired services to users. Network elements are usually considered to be those individual systems that provide the ultimate services to users or customers that lead to access to valuable system resources and information in the elements, while user elements are primarily a user interface to the network and used for access and unload of network resources and information. The communication sub-system that interconnects the user and network elements together are usually transparent to the users of the network resources and information. Therefore, a network can be interpreted rather differently depending on who the users are and what the network elements are. For example, regular users of an electronic mail service may not be aware of the existence of the routers in the network that are needed to route the mail traffic, nor do they care about their existence as long as the electronic mail can be correctly delivered as required and specified. On the other hand, network systems administrators have to deal with the configuration and management of routers to ensure seamless flow of network traffic. Therefore, to network systems administrators, routers are also network elements that need to be properly maintained.

As the result, in the abstraction of a networking environment, a network of individual systems can be modeled as being comprised of user elements **102**, network elements **104**, and the interconnection network **106**, as shown in FIG. **1**.

In the network of FIG. **1**, a user element is a local system accessible to the user in order for the user to access network resources and information that reside in the network elements. This abstracted network model allows the addressing of security concerns separately for the user elements and for the network elements although there might have some common concerns. It also helps focus on the network elements as the primary subject of discussion for security protection against unauthorized usage, disclosure, modification and destruction of network resources and information. In the case that a network element **104** is also a user element **102** to allow local user access, this abstraction requires the separation of the two logical functions, i.e., network service function and the user interface function. This separation does not have to be physical, however, but only indicates different functionality in the same network element. Eventually, the integration of local access control (described below) and remote network access control will make this distinction less meaningful, which is the ultimate goal of controlling access to the network elements.

1.2. Enterprise Network

A network for a business enterprise connects various network elements and employee office personal computers together. Network elements connected to the network can include switches, signaling transfer points (STPs), data access points (DAPs), mainframe computers, etc., that represent essential resources and information to conduct and succeed in business. A user is allowed to access a network element from a personal computer provided that the user has been granted the access right. To the user, the network is transparent in the sense that there is no need for the user to understand its internal structure, e.g., the way in which data packets are routed. All it needs for the user to access the network elements is a protocol for the personal computer and a network element to communicate with each other. It